NERC CIP -003-3 R5
Identify Individuals who can <u>authorise</u> access

SIEMENS

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

NERC CIP -003-3 R6
Changes to IED Firmware version
Changes to IED Configuration version and setting

SIEMENS

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

identify, control and document all entity or vendor-related changes to hardware and software components

NERC CIP 004-3a R4
Know who has access to what
Revoke <24 hours if dismissed
Revoke <7 days if access no longer required

SIEMENS

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

- Review quarterly, update list within 7 days
- Revoke access
- within 24 hours terminated with cause
- 7 calendar days no longer require access

SIEMENS

Not just power industry – any IED environment

- Utilities: power, water, gas, telecommunications;
- Transport control systems: road, rail, airport;
- Mining and/or industrial plant;
- Building/site management systems

- Smart Grid deployment
- Communicating sensors & controllers
- Cloud computing approaches
- Remote access to devices
- Smart phone access
- Wireless technology
- The "internet of things"

SIEMENS

Access for who? For what?

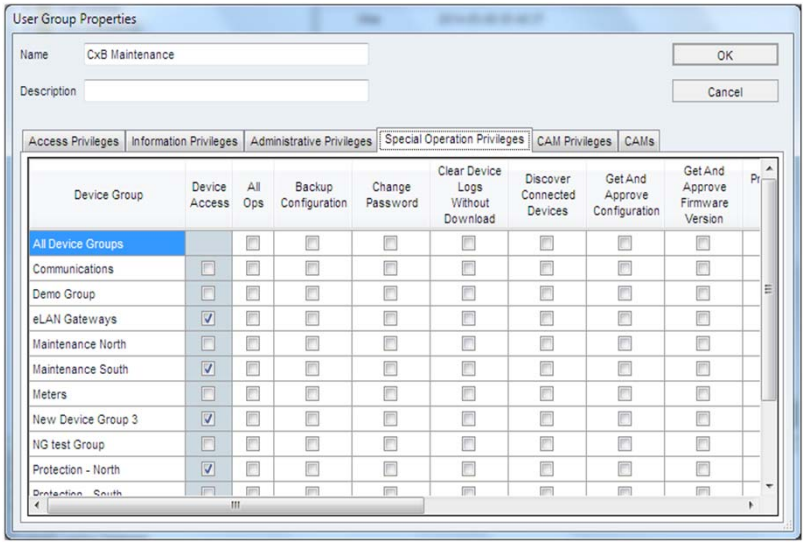
- Engineering personnel
- Commissioning personnel
- Maintenance personnel
- Vendor support personnel

- Geographical region
- Site specific
- Device Specific
- Command Specific
- Role Specific: View or Edit

Summary

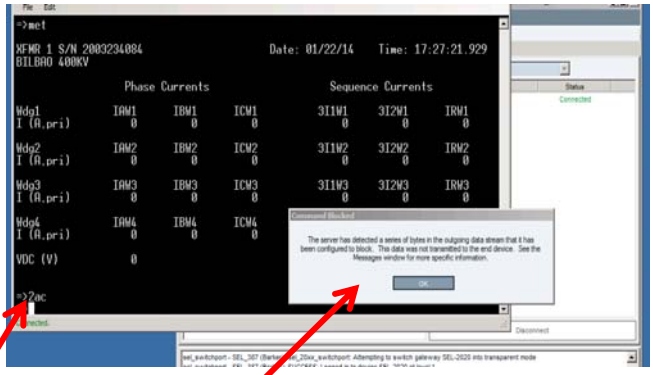
- Resilient central and remote architecture
- Centrally managed Users
- Comprehensive user-specific RBAC mechanisms
- IED-type agnostic operation
- Enhanced management of 'integrated' IED
- Centrally accessed with IED password obfuscation

Who needs access?



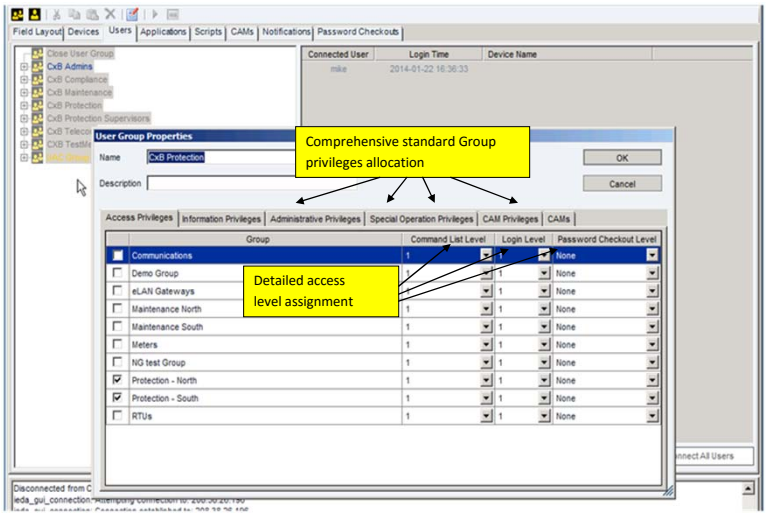
SIEMENS

To do what by whatever means



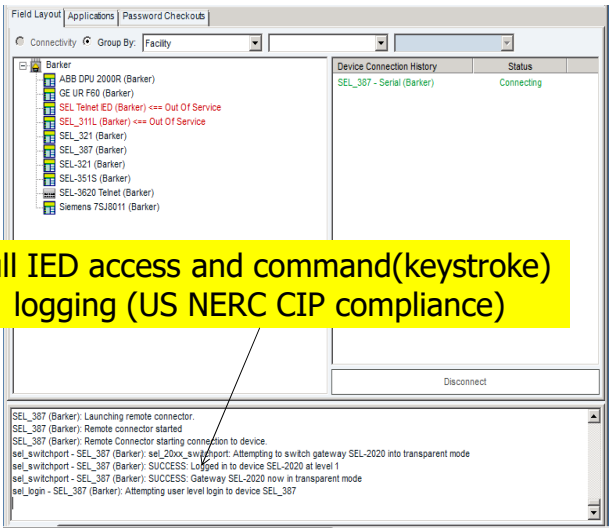
Full RBAC control at individual command level even if native IED software does not support RBAC

SIEMENS



SIEMENS

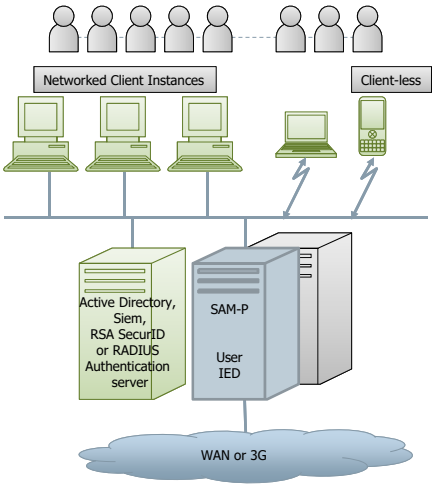
What have they done?

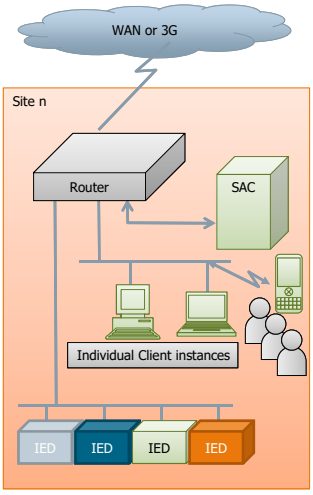


Full IED access and command(keystroke) logging (US NERC CIP compliance)

SIEMENS

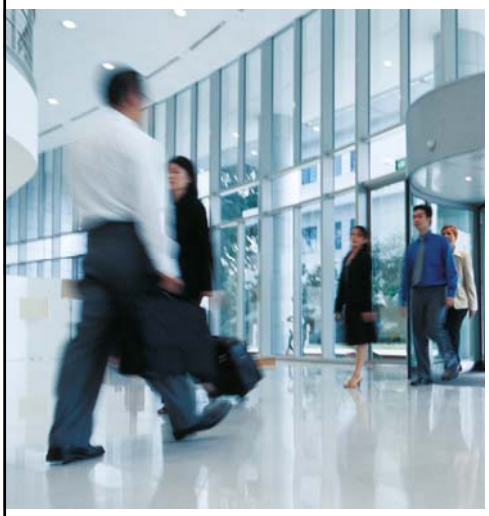
Architecture





SIEMENS

Further Information



Rodney Hughes
Business Development Manager
Industry / AU / IA SC

27 Greenhill Rd
Wayville
SA 5034
Australia

Mobile: +61 437 911 594

E-mail:
rodney.hughes@siemens.com

siemens.com/answers